Testimony from Verified Voting
To the Committee on GOVERNMENT ADMINISTRATION AND ELECTIONS
Connecticut General Assembly, regarding:

Proposed Bill No. 283
AN ACT CONCERNING ON-LINE VOTING FOR MILITARY PERSONNEL STATIONED OUT OF STATE

11 February 2013

OPPOSITION TO BILL NO. 283 – DON'T DISHONOR OUR MILITARY PERSONNEL WITH INSECURE VOTING

Chairs Musto and Jutila and Members of the Committee, Verified Voting works tirelessly around the country and in Washington D.C. to support expanded opportunities for our military personnel to vote. However we oppose Bill No. 283 because it would dishonor our military personnel with an insecure means to vote. Those serving to secure our democracy should not be provided an unequally insecure means to participate in that democracy. That is what 283 would do.

Verified Voting was a strong supporter of the federal MOVE Act, passed in October 2009. The MOVE Act continued to show excellent gains in voter enfranchisement amongst military personnel in the 2012 General Election.[1] We are members of the Alliance for Military and Overseas Voting Rights (AMOVR), where we join many military personnel support colleagues to work on their behalf year round.

We take support for military voting seriously and oppose 283 on strict empirical grounds of insecurity.

We strongly recommend against allowing ballots to be cast online, via email, internet-based fax, or through internet portals. Online voting presents a direct threat to the integrity of elections in Connecticut, because it is not sufficiently secure against fraud or malfunction. Cyber security experts with the Department of Homeland Security have publicly warned against internet voting.[2]

---

[1] OVF AND US VOTE 2012 POST-ELECTION SURVEY REPORT, A Detailed Look at How Voters and Election Officials Fared in the 2012 General Election and What To Do About It, https://www.overseasvotefoundation.org/files/OVF_ElectionReport_2013_web.pdf

[2] NPR, Pam Fessler: Online Voting 'Premature,' Warns Government Cybersecurity Expert, http://www.npr.org/blogs/itsallpolitics/2012/03/29/149634764/online-voting-premature-warns-government-cybersecurity-expert

In May 2012, the National Institute of Standards and Technology (NIST) published a statement strongly cautioning against voting over the internet, including via email.[3] In a published statement over 30 computer security experts and technologists warned against the use of the internet for this purpose.[4]

The problem is that security tools currently commercially available are inadequate to protect ballots cast online from corruption (intentional or otherwise). Indeed, even the most robust security tools available have been unable to stop attackers intent on breaching the most fortified government and corporate networks. Banks, despite very large budgets to build the most complex cyber defenses, lose billions a year to fraud and security breaches.[5] But banks budget these losses as a cost of doing business. We cannot make the same calculus with votes.

When Congress passed the MOVE Act to improve military and overseas voting, it did not authorize or mandate states to allow for the casting of marked ballots via email, internet-based fax or internet portal because the security risks are not yet solved – and because the other provisions of MOVE, if fully implemented, will make a huge difference in the ability of overseas and military voters to cast an effective ballot, even without resorting to electronic transmission of votes over the internet. Indeed, that is what the accumulating survey data is confirming – that these low-tech, secure improvements to military personnel enfranchisement are paying significant dividends.

Allowing ballots to be cast by email, internet-based fax, or through internet portals - at least with the current security tools - is an invitation to partisan operatives and nation-states to tamper with the integrity of our elections. The problem is particularly pernicious because it is unlikely that such attacks will be detected. Attacks on consumer and business bank accounts can be detected because the accounting systems are reviewed by multiple parties and auditable records exist. Bank statements, unlike our voted ballots, are not anonymous. This makes it critical that the physical ballot which the voter inspected is returned for counting. If a purely electronic form is transmitted, that unsecured vote is not verifiable by the voter and does not constitute an auditable record of the vote.

As the federal agency responsible for leading the development of voting system standards for the U.S. Election Assistance Commission, NIST has been tasked to research online voting systems. NIST is also charged to develop guidelines to be used by the Department of Defense for the creation of a secure online voting system for the military.

We therefore urge you to recommend that any legislation to allow internet voting require that NIST first establish standards for secure online voting and that any system under consideration for use in Connecticut be tested by a NIST accredited laboratory, that the system meet or exceed the NIST standards, and that the test reports be available to the public. We also encourage you to require that any online voting system under consideration for use in Connecticut undergo a security evaluation and

[3] http://www.nist.gov/itl/vote/uocava.cfm

[4] http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf

[5] http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf

penetration test by the Department of Homeland Security Cyber Security National Protection and Programs Directorate.

We look forward to any opportunity to work with Connecticut to improve the voting process for military and overseas voters. Please don't hesitate to contact us if we can answer any questions on this matter.

Very truly yours,

Dan McCrea
Verified Voting
dan@verifiedvoting.org
Cell: 305-984-2900